ไวรัสกับดอสตัวใหม่

เอนก ศิรจริยาภิวัฒน์

หลายคนคงสงสัยว่า บทความคราวนี้เป็นอะไรกันแน่ ไวรัสไปเกี่ยวข้องอะไรกับดอสตัวใหม่ สาเหตุที่เขียนบทความนี้เพื่อให้เรารู้จักการทำงานของไวรัสมากขึ้น เพื่อจะหาวิธีการป้องกันและแก้ไขได้ถูกต้อง สำหรับคำว่าดอสตัวใหม่นั้นเป็นสิ่งที่เราจะมาดูการทำงานของบูตเรคอร์ด (Boot Record) ว่าทำงานอย่างไร สำหรับคนที่กำลังศึกษาระบบจัดการ (OS) เพื่อที่จะได้นำระบบจัดการที่เขียนขึ้นเองเข้าสู่ระบบ (มิใช่นำไวรัสเข้าสู่ระบบนะครับ)

ไวรัส ทุกคนรู้จักคำนี้กันเกือบทุกคน (แม้ไม่ใช่นักคอมพิวเตอร์ยังรู้จัก) เพราะฉะนั้นเราจะไม่กล่าวรายละเอียดมากนัก พูดรวม ๆ แล้ว ไวรัส ก็คือ โปรแกรมที่สามารถแพร่ไปที่ต่าง ๆ โดยเราไม่ปรารถนาให้เจ้าตัวไวรัสทำงานเหล่านั้นเลย โดยไวรัสอาจทำให้ระบบหยุดทำงาน มีลักษณะผิดปกติ ทำลายแผ่นดิสค์ ทำลายข้อมูล อื่น ๆ อีกมาก แล้วแต่ผู้เขียนไวรัสจะปรารถนาให้ทำอะไร

การทำงานของบูตเรคอร์ด

โปรแกรมในส่วนของบูตเรคอร์ดจะเก็บที่ แทร็ก 0 เซกเตอร์ 1 ทำหน้าที่นำระบบจัดการ (OS) ลงสู่หน่วยความจำ เพื่อให้ระบบจัดการนั้นทำงานต่อไป โปรแกรมในบูตเรคอร์ดจะถูกโหลดโดย BIOS อีกทีหนึ่ง เมื่อเรารู้การทำงานของบูตเรคอร์ด เราก็สามารถนำระบบจัดการใด ๆ เข้าสู่ระบบได้ทั้งนั้น เราเคยเห็นเอกสาร วารสาร และหนังสือที่เขียนเกี่ยวกับระบบจัดการ เราคงได้มีโอกาสลองเล่นระบบจัดการนั้น ๆ ได้แล้วนะครับ เมื่อเรานำระบบจัดการใด ๆ ใส่ในแผ่นดิสค์ของเรา เราก็สามารถจัดโครงสร้างของดิสค์เสียใหม่ได้โดยไม่จำเป็นต้องตามรูปแบบอินเทล (intel format) เราก็หวังว่าเราอาจจะมีระบบจัดการภาษาไทยใช้กันบ้าง อาจจะเป็น TDOS หรือ TNIX ก็ได้ เพื่อเยาวชนไทยได้มีโอกาสมากขึ้นอีก หรือบางท่านอาจนำเทคนิคต่าง ๆ มาลองทำดิสค์ป้องกันการก๊อบปี้ (copy protect) ก็ได้ เราเริ่มมาดูตัวอย่างโปรแกรมในบูตเรคอร์ดดังรูปที่ 1 กันเลย โปรแกรมหลักจะเริ่มจากการพิมพ์ตัวเลข 1 บนจอเพื่อแสดงว่าบูตเรคอร์ดเริ่มทำงาน ต่อจากนั้นจะเริ่มย้ายตัวเอง (move-self) เพื่อป้องกันการโหลดระบบจัดการมาทับโดยไม่ตั้งใจ เพราะเราไม่รู้ว่า BIOS แต่ละเครื่องจะโหลดโปรแกรมบูตเรคอร์ดไว้ที่ใด (ปกติจะอยู่ที่ 0000:7C00) ถ้าเรารู้ว่า BIOS โหลดโปรแกรมบูตเรคอร์ดไว้ที่ใด เราก็ไม่จำเป็นต้องทำการย้ายโปรแกรมขณะปฏิบัติงาน เมื่อย้ายตัวเองเสร็จแล้ว ก็จะทำการอ่านดิสค์ที่แทร็ก 1 เซกเตอร์ 1 เพื่อนำโปร-

รูปที่ 1 โปรแกรมที่เก็บบนบูตเรคอร์ด

```
;-------------------------------------------------------
; Program : boot.asm
; Purpose : Show,how boot record work ?.
; Written : 27/7/89
; Last Update : 27/7/89
; Written By : Anek Sirajariyapiwat
;-------------------------------------------------------

ClrScr  MACRO
                Mov     Ah, 06h   ;function
                Mov     Al, 00h   ;clear screen
                Mov     Cx, 0     ; uper left
                Mov     Dh, 24    ; lower right
                Mov     Dl, 79
                Mov     Bh, 07h   ; attribute
                Int     10h       ;BIOS
        ENDM
;-------------------------------------------------------
GotoXY MACRO  X,Y
                Mov     Dl,X
                Mov     Dh,Y
                Mov     Ah, 02h
                Mov     Bh, 0
                Int     10h
        ENDM
;-------------------------------------------------------
Readkey Macro
                Mov     Ah,0
                Int     16h
        EndM
;-------------------------------------------------------
PutCh Macro X,Y,Ch
```

```
                GotoXY  X,Y,Ch
                Mov     Ah,09h
                Mov     Al,Ch
                Mov     Bx,07h
                Mov     Cx,10
                Int     10h
        EndM
;---------------------------------------------------------------

;---------------------------------------------------------------
; text attribute
;---------------------------------------------------------------
Normal      equ  07h
;---------------------------------------------------------------



;---------------------------------------------------------------
; locate of boot routine
;---------------------------------------------------------------
BOOT_SEG            segment at 50h                          ; select your self
                    org 0h
BOOT_OFF            label far
BOOT_SEG            ends
;---------------------------------------------------------------
BOOT_Size           equ     512d
BOOT_Stack          equ     7C00h
;---------------------------------------------------------------
; Your DOS parameter
;---------------------------------------------------------------



DOS_SEG             segment at  60h                         ; select your self
                    org 100h
DOS_OFF             label far
DOS_SEG             ends
;---------------------------------------------------------------
Time_to_read        equ     5
DOS_Size            equ     5                               ; Number of sector
DOS_Disk            equ     0101h                           ; Dos at Track 1,Sector 1
DOS_Stack           equ     0F000h
;---------------------------------------------------------------

;---------------------------------------------------------------
            Cseg segment
            Assume Cs:Cseg,Ds:Cseg
;---------------------------------------------------------------
;               < Main Program Here >
;---------------------------------------------------------------
Main                proc    near
Start:
                    clrscr
                    PutCh   10,9,'1'
                    ReadKey
                    Cli                                                    →
```

```
Move_self:
                Mov     Cx,BOOT_Size                            ; Size of BOOT routine
                Xor     Ax,Ax
                Mov     Ss,Ax
                Mov     Sp,Boot_Stack
                Mov     Ax,BOOT_SEG
                Mov     Es,Ax                                   ; BOOT routine target
                Mov     Di,offset  BOOT_OFF
                Push    Cs
                Pop     Ds
                Call    Begin_Move                              ; Save current IP
Begin_Move:
                Pop     Si                                      ; Get current IP

                Add     Si,((offset BOOT_routine)-(offset Begin_Move))  ; Next adjust source (SI)
                Rep     Movsb
                Jmp     BOOT_OFF
BOOT_routine:
                PutCh   10,10,'2'
                Readkey
                Mov     Cx,Time_to_read                         ; Retry times
Retry_read:
                Push    Cx
                Xor     Ax,Ax
                Sub     Dx,Dx                                   ; Drive 0 Head 0
                Int     13h                                     ; Reset Disk
                Mov     Ax,DOS_SEG
                Mov     Es,Ax
                Mov     Bx,offset DOS_OFF
                Mov     Ah,02h                                  ; Read funtion
                Mov     Al,DOS_Size
                Mov     Cx,DOS_Disk
                Int     13h                                     ; Disk Service
                Pop     Cx
                Jnc     Read_OK
                loop    Retry_Read
                Jmp     Read_ERROR
Read_OK:
                Cli

                Mov     Ax,DOS_SEG
                Mov     SS,Ax
                Mov     SP,DOS_Stack
                Sti
                Jmp     DOS_OFF
Read_ERROR:
                PutCh   10,11,'3'
                Readkey
                int     19h
;---------------------------------------------------------------
Main            EndP
;---------------------------------------------------------------
          Cseg EndS
               End Start
```

แกรมระบบจัดการตัวอย่าง (DOS.COM) ลงสู่หน่วยความจำ (เก็บที่ track 1 sector 1 หรือที่อื่นก็ได้) หน่วยความจำส่วนนี้สามารถระบุเองได้ แต่ห้ามทับโปรแกรมบูตเรคอร์ด เพราะโปรแกรมบูตเรคอร์ดยังทำงานไม่สำเร็จ เมื่อโหลดระบบจัดการเสร็จ เราก็จะกระโดด (JUMP) ไปที่แอดเดรสที่เก็บระบบจัดการนั้น เพื่อส่งการทำงานให้ระบบจัดการต่อไป การเขียนโปรแกรมมีข้อระวัง ก็คือ การย้ายตัวเองของโปรแกรมบูตเรคอร์ด และการโหลดระบบจัดการ ห้ามระบุแอดเดรสที่ตรงกับตารางอินเตอร์รัพต์เวกเตอร์ (ยกเว้น อินเตอร์รัพต์นั้นไม่ใช้โดย BIOS) อีกข้อหนึ่งก็คือ โปรแกรมที่เขียนขึ้นมาห้ามใช้ฟังก์ชัน MSDOS เพราะยังไม่มีการทำงานของดอสตัวใด ๆ ทั้งสิ้น หวังว่าเราคงมีระบบจัดการของตัวเราเองนะครับ การนำโปรแกรมทั้งสองเก็บลงดิสค์ ใช้ Norton utility หรือ debug.com หรือเขียนโปรแกรม format แล้วเขียนโปรแกรมลงไปเองก็ได้

ไวรัสที่อยู่บนบูตเรคอร์ด

ไวรัสประเภทนี้ตัวแรกที่เราคุ้นหูก็คงเป็น Pakistani Brain Virus ((c) Brain)ไวรัสประเภทนี้ เมื่อเรารู้การทำงานของบูตเรคอร์ด เราก็สามารถรู้การทำงานของไวรัสเหล่านี้ได้ ไวรัสเหล่านี้อาจนำบูตเรคอร์ดเดิมไปไว้ที่อื่นของแผ่นดิสค์หรือเขียนทับบูตเรคอร์ดนั้นเลย

การค้นหา

ปกติจะใช้การดูบูตเรคอร์ด ถ้าพบว่าบูตเรคอร์ดไม่มียี่ห้อของโปรแกรมที่ใช้ format เช่น IBM, MSDOS หรือ pctools ให้สงสัยไว้ก่อนว่าเป็นแผ่นไวรัส ให้เช็คไบต์ที่ 0-9 กับไวรัสที่รู้จักอยู่ ถ้าไม่เจอให้พยายามหาว่าใช้โปรแกรมอะไรฟอร์แมตดิสค์แผ่นนั้น ผลที่ฟอร์แมตออกมาบูตเรคอร์ดเหมือนกันหรือไม่ ถ้าไม่เหมือนหรือหาโปรแกรมที่ใช้ format ไม่เจอให้ก๊อบปี้บูตเรคอร์ดจากแผ่นที่แน่ใจว่าไม่มีไวรัสทับลงไป ส่วนแผ่นที่ยี่ห้อถูกต้องก็ขอให้เช็ค 2-3 ไบต์แรก ซึ่งเป็นคำสั่ง JUMP ว่าถูกต้องหรือไม่ (เทียบกับแผ่นที่ใช้โปรแกรม format เดียวกัน) ถ้าเป็นการบูตเครื่องให้สังเกตว่า ถ้าบูตครั้งแรกไม่สำเร็จให้ลองบูตอีกครั้ง (ด้วยแผ่นเดิม) สังเกตว่ามียี่ห้อของ BIOS ขึ้นมาหรือไม่ ถ้าไม่ ให้สงสัยไว้ก่อน (พบในไวรัสชื่อ 1 K) หรือบูตแล้วมีข้อความแปลก ๆ เสียงประหลาด ๆ หรือ CAPLOCK, NUMLOCK, SCROLLLOCK ที่กดไว้ไม่ได้รับการรีเซต ให้สงสัยว่าแผ่นเป็นไวรัส ให้เช็คแผ่นนั้นกับแผ่นปกติซะ

การแก้ไข

ถ้าเป็นแผ่นดอสให้ใช้ sys.com จากแผ่นที่ไม่มีไวรัส ถ้าไม่ใช่แผ่นดอสให้ใช้โปรแกรมยูทิลิตี้ เช่น Norton Utility, PC Tools ก๊อบปี้บูตเรคอร์ดทับลงไป หรือท่านที่มีฮาร์ดดิสค์และ debug.com ให้ก๊อบปี้จากฮาร์ดดิสค์โดย

```
L 0 2 0 1
W 0 0 0 1
Q
```

ถ้ามีคลัสเตอร์ บางครั้งคลัสเตอร์ถูกแปลงเป็นคลัสเตอร์เสีย (พบใน (c) Brain) ให้แก้เป็นคลัสเตอร์ที่ดอสมองเห็นด้วย

การป้องกัน

การป้องกันนั้นมีหลายรูปแบบ ซึ่งมีคนนำเสนอมากมาย ส่วนการป้องกันที่จะแนะนำ เป็นความคิดเห็นของผู้เขียนเอง

1. ใช้โปรแกรม format อยู่บริษัทเดียว เพื่อจะได้รู้ว่าบูตเรคอร์ดของเราเป็นอย่างไร

2. หมั่นตรวจบูตเรคอร์ดโดยโปรแกรมยูทิลิตี้ต่าง ๆ หรือท่านที่มี debug.com ก็ใช้ debug.com หรือจะเขียนแบตช์ไฟล์ตอนบูตระบบได้ดังรูปที่ 2

Drive	A	C
ไฟล์คำสั่ง	ชื่อ BOOT.DAT บรรจุ L 0 0 1 D 0 , 1FF Q	ชื่อ BOOT.DAT บรรจุ L 0 2 0 1 D 0, 1FF Q
แบตช์ไฟล์	ชื่อ BOOT.BAT บรรจุ ECHO OFF DEBUG <BOOT.DAT	ชื่อ BOOT.BAT บรรจุ ECHO OFF DEBUG <BOOT.DAT

รูปที่ 2 ลักษณะแบตช์ไฟล์ของการบูตระบบในไดรฟ์ A และ C

3. สำหรับท่านที่มีฮาร์ดดิสค์ให้บูตจากฮาร์ดดิสค์ตลอด ถ้าไม่มีฮาร์ดดิสค์ ให้ทำแผ่นดอสไว้ 2 แผ่นหรือมากกว่า (กันเสีย) ติด write protect ทุกแผ่นด้วย แล้วบูตด้วยแผ่นดอสเหล่านี้ ถ้าเผลอบูตระบบด้วยแผ่นอื่น แม้จะไม่ใช่แผ่นดอส ให้ปิดเครื่องแล้วเริ่มกันใหม่

4. เขียนโปรแกรม CRC หรือเช็ค sum ของบูตเรคอร์ด แล้วบรรจุโปรแกรมนี้ไว้บน AUTOEXEC.BAT

5. หลอกให้ไวรัสคิดว่ามีตัวไวรัสอยู่แล้ว เช่น (c) Brain จะเช็คไปตัวที่ 4 ว่าเป็น 1234 หรือไม่

ไวรัสที่เกาะกับโปรแกรมอื่น

ไวรัสประเภทนี้น่ากลัวกว่าประเภทแรก เพราะสามารถกระจายโดยไม่มีขอบเขตจำกัด ยิ่งเป็นระบบ LAN ยิ่งไปได้สะดวก นั่นคือยิ่งมีการใช้คอมพิวเตอร์ร่วมกันมากเท่าไร โอกาสที่จะติดไวรัสก็จะมากตาม

การค้นหา

สังเกตการทำงานของโปรแกรมผิดปกติไปหรือไม่ เช่น มีแท่งดำ ๆ ในเท็กซ์โหมด หรือแท่งสีอื่นในกราฟิกโหมด การทำงานช้าลง (พบในอิสลาเอล sUMsDos ไวรัสตัวนี้จะทำให้การทำงานของระบบช้าลงเมื่อไวรัสเริ่มทำงานไปแล้วประมาณ 30 นาที) มีตัวอักษรหรือเสียงประหลาด ๆ เกิดขึ้น จอดับไปเฉย ๆ ขนาดของโปรแกรมใหญ่ขึ้น ให้สังเกต command.com ด้วย เพราะไวรัสบางตัวติดที่ command.com

การแก้ไข

ถ้ารู้ว่าเป็นไวรัสชนิดใด เพิ่มขนาดโปรแกรมเท่าไร เกาะที่ส่วนใดของโปรแกรม เราก็สามารถกำจัดมันได้ไม่ยาก เช่น sUMsDos ที่เราคุ้นเคยอยู่ตอนนี้ติดกับไฟล์นามสกุล .com ติดกับส่วนบนของโปรแกรม กินขนาด 1813 ไบต์ เราก็ตัดส่วนนี้ออก ไฟล์นามสกุล .com นี้ จะติดไวรัส sUMsDos ครั้งเดียว ส่วน .EXE จะติดได้หลายครั้ง แต่ละครั้งจะเพิ่มขนาดขึ้น 1808 ไบต์ การแก้ไขก็โดยการเช็คว่าติดไวรัสไปกี่ครั้ง แล้วตัดโปรแกรมออกด้วยขนาด 1808 คูณด้วยจำนวนครั้งที่ติดไวรัส เสร็จแล้วแก้ Header ของ .EXE ไบต์ที่ 2-3 และไบต์ที่ 16-23 ให้เริ่มต้นการทำงานของโปรแกรมให้ถูกต้องด้วย

การป้องกัน

1. คอยเช็คว่ามีโปรแกรม TSR โดยไม่ตั้งใจเกิดขึ้นหรือไม่ ? ดังรูปที่ 3 และ 4 หรือเขียนโปรแกรม TSR คอยเช็คหน่วยความจำว่ามีไวรัสหรือไม่ ? ปกติโปรแกรม TSR นี้จะใช้อินเตอร์รัพต์ 1C เพื่อที่จะทำงานได้ตลอดเวลา การเช็คก็โดยดูอินเตอร์รัพต์เวคเตอร์ ว่าชี้ไปยังที่มีไวรัสอยู่หรือไม่ ? เช่น sUMsDos ใช้อินเตอร์รัพต์เบอร์ 21h กับ 8h (ให้สังเกตด้วยว่า sUMsDos นี้ใช้หน่วยความจำ 1792 ไบต์)

2. เขียนโปรแกรมเก็บตารางอินเตอร์รัพต์เวคเตอร์แล้วเช็คว่าอินเตอร์รัพต์เวคเตอร์เปลี่ยนไปหรือไม่ โปรแกรมนี้ต้องเริ่มใหม่เมื่อใช้โปรแกรมที่เปลี่ยนอินเตอร์รัพต์เวคเตอร์ด้วย

```
Allocated Memory Map - by TurboPower Software - Version 2.6

 PSP   blks  bytes  owner     command line          hooked vectors
-----  ----  -----  --------  --------------------  ------------------------------
0008     1   16432  config                          22 2E
00BF     2    4576  command                         08 09 10 13 1C 21 25 26 CE
0EF8     2  104928  SK                              CF DD DE F0 F3 F5 FD FF

2898     2   72112  NG                              16 28
3A36     2  416928  free
```

รูปที่ 3 หน่วยความจำเมื่อ sUMsDos ยังไม่ทำงาน

```
Allocated Memory Map - by TurboPower Software - Version 2.6

 PSP   blks  bytes  owner     command line          hooked vectors
-----  ----  -----  --------  --------------------  ------------------------------
0008     1   16432  config                          22 2E
00BF     2    4576  command                         09 10 13 1C 25 26 CE CF DD
0EF8     2  104928  SK                              DE F0 F3 F5 FD FF

2898     2   72112  NG                              16 28
3A35     1    1792  N/A                             08 21
3A8C     2  414784  free
```

รูปที่ 4 หน่วยความจำเมื่อ sUMsDos ทำงานแล้ว

เช่น SK การจะรู้ว่าโปรแกรมใดใช้อินเตอร์รัพต์เวคเตอร์ต้องเก็บตั้งแต่ได้โปรแกรมนั้นมาใหม่ ๆ และแน่ใจว่าไม่เป็นไวรัสเก็บไว้เป็นข้อมูลสำหรับโปรแกรมเช็คตารางอินเตอร์รัพต์เวคเตอร์ที่เราสร้างขึ้นมา

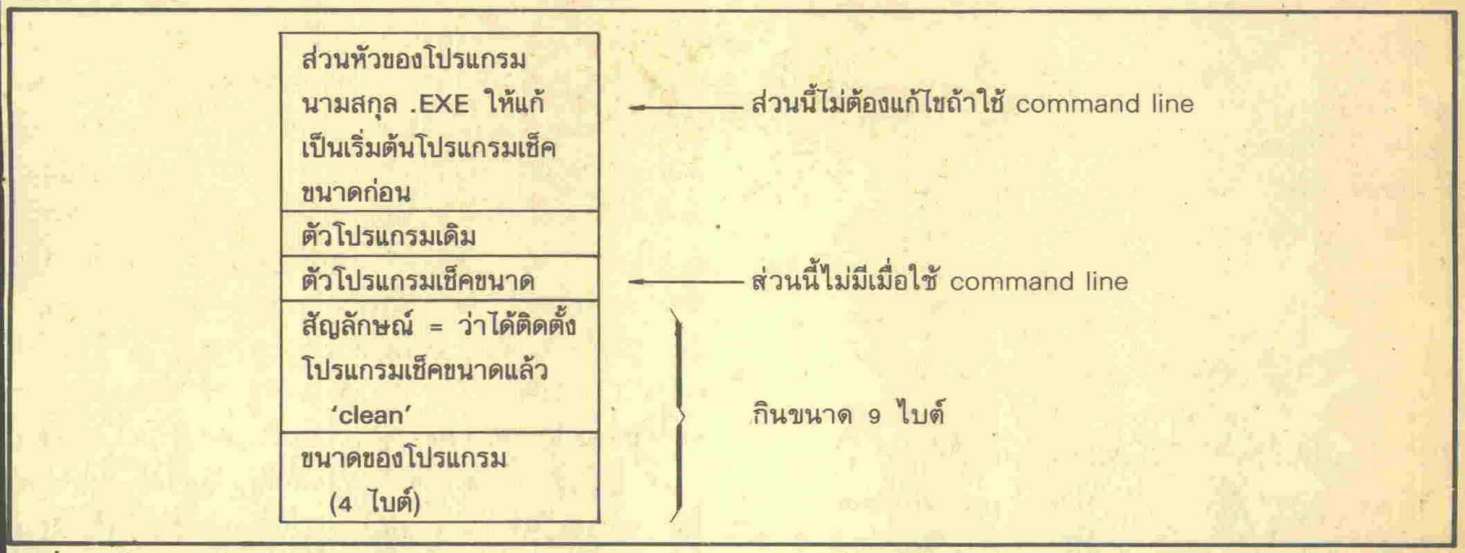
3. เขียนโปรแกรมเช็ค CRC หรือ check sum ของโปรแกรมต่าง ๆ ว่าเปลี่ยนไปจากเดิมหรือไม่

4. เขียนขนาดของโปรแกรมลงไปบนโปรแกรมนั้น ๆ เลย แล้วเขียนโปรแกรมเช็คขนาดติดกับโปรแกรมนั้น ๆ เลย ดังรูปที่ 5 เมื่อเริ่มทำงานให้เริ่มการเช็คขนาดก่อน ถ้าขนาดเปลี่ยนไปก็จะหยุดการทำงาน เพื่อไม่ให้ไวรัสแพร่ระบาดได้ การเขียนโปรแกรมเช็คขนาดนี้ จำเป็นต้องมีข้อความแสดงว่าโปรแกรมได้เริ่มทำงานแล้ว มิฉะนั้นถ้าไวรัสเปลี่ยนจุดเริ่มต้นของโปรแกรม เราจะไม่สามารถรู้ได้เลยว่าโปรแกรมเราจะทำงานหรือไม่ ? การเขียนโปรแกรมเช็คขนาดนี้อาจเขียนแยกไว้ต่างหาก โดยบรรจุขนาดและสัญลักษณ์ว่าโปรแกรมนี้ได้

ในคราวหน้า โปรแกรมลักษณะนี้มีข้อเสีย คือ โปรแกรมเดิมมีขนาดใหญ่ขึ้น แต่ก็ยังดีกว่าใหญ่ขึ้นเพราะไวรัส การเขียนโปรแกรมเช็คขนาด เช็ค CRC และ check sum นี้ ควรใช้กับ command.com ตอนเริ่มระบบด้วย

การป้องกันไวรัสมีอีกมากมาย ซึ่งแล้วแต่ว่าเราจะใช้วิธีใด หนึ่งในวิธีเหล่านั้น คือใช้โปรแกรมเช็คไวรัส เราควรจะรู้ว่าโปรแกรมมาจากที่ใดเพื่อกันโปรแกรมเช็คไวรัสเข้าข่ายโปรแกรมประเภทม้าโทรจัน คือหลอกให้ผู้ใช้เข้าใจผิด แท้ที่จริงตัวโปรแกรมเองเป็นตัวทำลายระบบ ขอให้ระวังด้วยนะครับ

5. ถ้าใช้โปรแกรมที่มีการเก็บข้อมูล เช่น dBase, LOTUS หรือโปรแกรมเวิร์ดโปรเซสซิ่ง มีข้อแนะนำว่า ให้ใส่แผ่นโปรแกรมที่ติด write protect ไว้ drive A แล้วนำแผ่นข้อมูลไว้ drive B โดย drive B ไม่ควรมีโปรแกรม .EXE หรือ .COM อยู่ด้วย



รูปที่ 5 ขั้นตอนของโปรแกรมเช็คขนาด

บรรจุขนาดแล้วในตัวอย่าง ผู้เขียนใช้คำว่า 'clean' ไว้ท้ายโปรแกรมที่ต้องการเช็คขนาดเท่านั้น ตัดตัวโปรแกรมเช็คขนาดออก แล้วสั่งผ่าน command line เหมือนสมัยที่เราใช้ apple กันนั่นเอง เช่น ต้องการเช็คขนาดของ TURBO.EXE โดยโปรแกรมเช็คคือ SIZE เราก็สั่งโดย

A>SIZE TURBO.EXE

เมื่อต้องการให้เทอร์โบปาสคาลทำงานก็สั่ง

A>RUN TURBO.EXE

โดยโปรแกรม RUN จะเป็นตัวเช็คขนาด สำหรับโปรแกรมในลักษณะนี้ผู้เขียนคิดว่าได้ผลมาก ซึ่งจะนำมาแสดง

มีอะไรใหม่

ไวรัสที่เรารู้จักกันดีก็คือ (c) Brain และ sUMsDos ตัวอื่นก็มี 1K, FAT ERASER, T2 ซึ่ง 3 ตัวหลังนี้อยู่กลุ่มเดียวกัน คราวนี้เรามาดูไวรัสที่ระบาดกันตอนนี้เพิ่มเติมบ้าง

1. Lehigh Virus

ไวรัสตัวนี้ติดกับ command.com โดยตัวไวรัสจะเปลี่ยนอินเตอร์รัพต์ 21h ไว้ที่ตัวไวรัสเอง แล้วเปลี่ยนโปรแกรมของอินเตอร์รัพต์เวคเตอร์ 21h ไว้ที่อินเตอร์รัพต์ 44h (ในเวอร์ชัน 2 ที่ถูกค้นพบในเดือนกุมภาพันธ์ใช้อินเตอร์รัพต์ 63h ด้วย) เมื่อไวรัสตัวนี้พบว่าตัวมันเองแพร่ขยายครบ 4 ครั้ง โดยถ้า

เป็นฮาร์ดดิสก์จะเขียนจำนวนครั้งไว้ที่ command.com ถ้าเป็นฟลอปปี้ดิสก์ หรือเป็น Lehigh เวอร์ชัน 2 จะเขียนจำนวนครั้งในหน่วยความจำเมื่อครบ 4 ครั้ง (ในเวอร์ชัน 2 เป็น 10 ครั้ง) ไวรัสตัวนี้ก็จะทำลายข้อมูล (trash) ในฮาร์ดดิสก์

2. ASHAR VIRUS

ไวรัสตัวนี้อยู่ติดกับ command.com เช่นเดียวกัน โดยใน command.com จะมีข้อความซ่อนอยู่ว่า "Welcome to the dungeon..." บางครั้งเลเบลก็ถูกเปลี่ยนเป็น ASHAR เช่นเดียวกับ (c) Brain จนมีผู้สงสัยว่าไวรัสตัวนี้พัฒนามาจาก (c) Brain นั่นเอง

3. Alameda VIRUS

มีผู้เขียนถึงไวรัสตัวนี้ในกรุงเทพฯเองคือ Gor don Willis โดยกล่าวไว้ว่า ไวรัสชนิดนี้จะทำให้จอมีขยะ (garbage) และมีเสียงดัง (bell rang) และดิสก์ที่เคยบูตได้จะไม่สามารถบูตได้อีก (คล้ายไวรัส 1K) จำนวนเนื้อที่ดิสก์ที่เสียเพิ่มมากขึ้น ปัญหาเหล่านี้จะเกิดขึ้นระหว่างการบูตระบบ โดยมีข้อสังเกตสำหรับไวรัสชนิดนี้คือ

3.1 เมื่อระบบติดไวรัสนี้แล้ว เมื่อทำการบูตจะไม่มีข้อความของบริษัทผู้ผลิต BIOS

3.2 คีย์ Capslock, Numlock หรือ ScrollLock ถ้าเดิมกดอยู่ (ON) จะไม่ได้รับการรีเซต

3.3 เมื่อใช้ CHKDSK.COM จะพบว่ามี hidden files เพิ่มขึ้นมา 1 ไฟล์ในแผ่นปกติของดอสจะมี 2 hidden file คือ IBMIO.COM และ IBMDOS.COM หรือ IO.SYS และ MSDOS.SYS ถ้าพบว่ามี 3 hidden files ก็ให้สงสัยไว้ก่อน

3.4 บูตเรคอร์ด ไม่มีชื่อของโปรแกรมที่ใช้ format

3.5 บางครั้งถ้าใช้โปรแกรมเรียง (sort) ไดเรคทอรีแล้วจะทำให้แผ่นไม่สามารถบูตได้

4. Screen Virus

ไวรัสตัวนี้จะติดกับไฟล์นามสกุล .com ที่อยู่ในไดเรคทอรีปัจจุบัน (current directory) ไวรัสตัวนี้จะใช้ timer tick เมื่อไวรัสทำงานมันจะเช็คจอภาพในตำแหน่งสุ่มขึ้นมา ถ้าพบว่ามีตัวเลข 4 ตัวเรียงกัน ก็จะทำการสลับตำแหน่ง 2 ตัว ไวรัสตัวนี้สังเกตได้ง่าย โดยจะมีข้อความ InFeCt ในโปรแกรมนั้น ๆ

5. dBASE VIRUS

ไวรัสตัวนี้คล้ายกับ sUMsDos คือเกาะติดกับโปรแกรมอื่น ไม่มีผลกับโปรแกรม dBASE โดยตรง แต่ตัวมันจะเปลี่ยนอินเตอร์รัพต์ 21h เพื่อคอยเช็คว่ามีการเปิดไฟล์นามสกุล .DBF หรือไม่ เมื่อเปิดไฟล์ .DBF ไวรัสตัวนี้จะเก็บขนาดของไฟล์ .DBF ไว้ เมื่อมีการเขียนกลับ ไวรัสตัวนี้จะทำการสลับ 2 ไบต์แรกของไฟล์นั้น หลังจากไวรัสเริ่มทำงาน 90 วัน มันก็จะทำลาย FAT ไวรัสตัวนี้จะสร้าง hidden file ชื่อ BUG.DAT เมื่อเราใช้ CHKDSK แล้วพบว่า hidden file เพิ่มขึ้น ก็ขอให้เช็คไฟล์ชื่อนี้ด้วย และถ้าเราสร้างไฟล์ BUG.DAT ขึ้นเองแล้ว ทำให้ไฟล์นี้เป็น read only ไวรัสตัวนี้จะไม่สามารถเปิดไฟล์ประเภท read only นี้ได้ มันจึงทำงานไม่ได้ ข้อมูลเราเลยปลอดภัย

6. FoxBase VIRUS

ไวรัสตัวนี้ถูกกล่าวถึงโดย Mare Holt ที่อยู่ในกรุงเทพฯนี้ โดยเขาก็อบปี้โปรแกรม Foxbase 2.0 จากอินเดีย แล้วนำมาติดตั้งในระบบ ปรากฏว่าเมื่อใส่รหัสผ่านเรียบร้อย เครื่องเกิดหยุดทำงาน (Hang up) จอภาพดับลง เขาจึงเริ่มระบบ (boot) ใหม่ สิ่งที่เขาสังเกตเห็นก็คือ เครื่องหมาย prompt ถูกเปลี่ยนจาก C เป็น E และเมื่อใช้ CHKDSK เขาพบไฟล์ที่เป็น hidden file เพิ่มขึ้น 1 ไฟล์มีขนาด 0 ไบต์ และเมื่อใช้ pctools เช็ค เขาก็พบคำว่า Ashar และใน command.com เขาก็พบข้อความว่า "Welcome to dungeon" โดยไฟล์ command.com จะถูกเปลี่ยนวันที่ด้วย เขาแก้ปัญหาโดยการฟอร์แมตฮาร์ดดิสก์ แต่เขาก็พบว่า ไวรัสดังกล่าวยังอยู่กับเขาอีก เมื่อเขาเริ่มต้นระบบให้แล้วพบอาการเช่นเดิม และเมื่อเขาใช้ Sidekick เพื่อทำเวิร์ดโปรเซสซิ่ง เมื่อผ่านไป 2 นาที จอภาพหดลงเหลือครึ่งนิ้ว จอภาพมีสโนว์ แล้วเครื่องก็หยุดทำงาน เรื่องของเขาก็จบลงเท่านี้ ซึ่งเป็นสิ่งที่แสดงว่า ASHAR ได้เข้ามาในกรุงเทพฯแล้ว ขอให้ระวังด้วยนะครับ โดยสังเกตจากอาการที่เล่ามา

7. ม้าโทรจัน

มีโปรแกรมลักษณะเดียวกันกับไวรัสอีก 2 ประเภทคือ

- ตัวหนอน จะเป็นโปรแกรมที่ทำลายโปรแกรมหรือข้อมูลโดยการเขียนข้อมูลลงไปกลางโปรแกรมที่จะทำลายโดยเขียนต่อกันไปเรื่อย ๆ คล้ายทางเดินของหนอน เช่น เขียน 0 ลงบนโปรแกรมต่าง ๆ จนโปรแกรมทำงานไม่ได้

- ม้าโทรจัน เป็นโปรแกรมที่ผู้ใช้รู้สึกสนใจในตัวโปรแกรมนั้นแล้วขอก็อบปี้ต่อไปเรื่อย ๆ อาจมาในรูปเกม โดยไม่รู้ว่าขณะโปรแกรมเหล่านั้นทำงาน มันได้เริ่มทำลายระบบไปพร้อม ๆ กันด้วย

เรามาดูตัวอย่างรายชื่อโปรแกรมม้าโทรจันกัน เพื่อเวลาเราเจอกับมัน จะได้ระวังตัวได้ทันก่อนที่เหตุการณ์จะสายเกินแก้ สำหรับโปรแกรมที่ไม่ระบุนามสกุล จะเป็นโปรแกรมที่พบในหลาย ๆ นามสกุล ดังรูปที่ 6

นอกนั้นยังมี ANTI-PCB, DMASTER, FINANCE 4.ARC, MAP, TIRED, QUIKRBBS.COM, QUIKREF STAR.EXE. STRIPES.EXE, TOPDOS และ VDIR.COM ให้ระวังโปรแกรมที่ทราบแหล่งที่มาด้วยนะครับ สุดท้ายก็ขอขอบคุณทุกท่านที่พยายามเขียนโปรแกรมป้องกันและแก้ไขไวรัส และขออวยพรให้ท่านที่เขียนไวรัส พบกับไวรัสที่ท่านเขียนและทำลายระบบของท่านเอง ขอให้ปลอดภัยทุกคน สวัสดีครับ

รูปที่ 6 หน้าที่ของโปรแกรมม้าโทรจันต่าง ๆ

โปรแกรม	หน้าที่
ARC513.EXE,ARC514	เมื่อทำงานจะทำงาน FAT ของ[ฮาร์ด]ดิสค์
BACKTALK	จะเขียนข้อมูลบนเซกเตอร์ของ[ฮาร์ด]ดิสค์ ทำให้ข้อมูลเสียไป
CDIR.COM	จะให้ไดเรคทอรีเป็นสี แต่ขณะเดียวกันจะทำลาย FAT ด้วย
DANCERS.BAS	จะมีรูปเต้นรำเป็นสี แต่จะทำลาย FAT ไปด้วย
DISKSCAN.EXE	จริง ๆ แล้วโปรแกรมนี้เขียนโดย PC-MAGAZINE แต่มีผู้แก้ไขให้เขียนข้อมูลผิด ๆ ลงบนเซกเตอร์ เราอาจเจอโปรแกรมนี้ในชื่ออื่น เช่น SCANBAD.EXE และ BADDISK.EXE ทำลาย FAT
DMASTER	
DOSKNOWS.EXE	มีคนเขียนโปรแกรมทำลาย FAT แล้วเปลี่ยนเป็นชื่อนี้ โดยตัวจริงมีขนาด 5376 ไบต์
DPROTECT	มีคนเขียนโปรแกรมทำลาย FAT โดยใช้ชื่อนี้เหมือนกับ DOSKNOWS
EGABTR	จะมีข้อความว่า "improve your EGA display"
EMMCACHE V1.0	ผู้เขียนโปรแกรมเขียนคู่มือประกอบไว้ด้วย แต่เมื่อติดตั้ง EMS disk cache ไป 69 หน้า จะทำลายข้อมูลในทุกไฟล์และทำลายบูตเซกเตอร์
FILER.EXE	โปรแกรมนี้มีตัวจริงอยู่ แต่ตัวที่เขียนขึ้นใหม่จะลายในฮาร์ดดิสค์ทั้งหมด (ผู้พบเจอปัญหากับฮาร์ดดิสค์ขนาด 20 Mbyte)
FUTURE.BAS	เมื่อให้โปรแกรมทำงาน จะมีรูปสีสวย ๆ ให้ดู แต่ขณะเดียวกันจะลบข้อมูลทุก drive ไม่ว่าจะเป็น drive A,B,C หรือ D ไม่ทำลายเฉพาะ FAT แต่จะลบไฟล์ทุกไฟล์ด้วย แต่จะลบเฉพาะไดเรคทอรีเดียว โดยไดเรคทอรีอื่น ๆ ปลอดภัย
NOTROJ.COM	โดยโปรแกรมทำให้ผู้ใช้เข้าใจว่าตัวมันเป็นตัวป้องกันโปรแกรมม้าโทรจัน โดยจะขึ้นข้อความว่า "another program is attempting a format, can't abort" แต่ตัวมันจะทำลาย FAT เมื่อทำลาย FAT จะเริ่มฟอร์แมตดิสค์ต่อไป ตัวจริงของโปรแกรมนี้เขียนโดย Jame H. Coombes แต่จะไฟล์อักษรชื่อ NOTROJ.TXT ถ้าไม่มีไฟล์นี้ให้ระวังไว้ด้วย
TSRMAP	ตัวโปรแกรมจะให้แผนที่หน่วยความจำของโปรแกรมประเภท TSR แต่ตัวมันจะทำลายบูต-เซกเตอร์ของ drive C
PACKDIR	เป็นตัวเรียงไดเรคทอรี แต่ตัวมันจะทำลาย FAT
RCKVIDEO	จะมีรูปของดาราร็อค (ผู้พบคิดว่าเป็น มาดอนน่า) แต่ตัวมันจะทำลายข้อมูลในฮาร์ดดิสค์ เมื่อเสร็จแล้วจะสร้างแอสกี้ไฟล์ 3 ไฟล์ โดยมีข้อความว่า "You are stupid to download a video about rock star," หรือข้อความทำนองนี้
SECRET.BAS	จะทำการฟอร์แมตดิสค์
SEX.EXE	จะขึ้นรูปที่น่าสนใจ แต่ก็จะเริ่มทำลายระบบไปพร้อม ๆ กัน
SIDEWAYS.COM	ตัวจริงจะเป็น .EXE มีขนาดประมาณ 30 Kbyte ตัว .COM นี้จะมีขนาด 3 Kbyte จะทำลายบูตเซกเตอร์